

15 $C_k \equiv M^{e_k} \pmod{p_k},$

16 where

17 $M_1 \equiv M \pmod{p_1},$

18 $M_2 \equiv M \pmod{p_2},$

19
20 $M_k \equiv M \pmod{p_k},$

22 $e_1 \equiv e \pmod{(p_1 - 1)},$

23 $e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$

24 \vdots

25 $e_k \equiv e \pmod{(p_k - 1)},$

27 where e is a number relatively prime to $(p_1-1), (p_2-1), \dots,$ and $(p_k-1),$

28 solving said subtasks to determine results $C_1, C_2 \dots C_k,$

29 combining said results of said subtasks in accordance with a fast recursive combining

30 process to produce said ciphertext word signal C whereby,

31 $Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1}) (w_i^{-1} \pmod{p_i}) \pmod{p_i}] \cdot w_i \pmod{n}$

32 $2 \leq i \leq k, \text{ and}$

33 $C = Y_k, Y_1 = C_1, \text{ and } w_i = \prod_{j < i} p_j$

34 whereby said step of encoding is accelerated.

1 15. (Three Times Amended) A method for establishing cryptographic communications that are
2 backwards compatible with preexisting public key transformation schemes, comprising the steps
3 of:

4 decoding a ciphertext word C to a message word M , wherein M corresponds to a number
5 representative of a message and wherein,

6 $0 \leq M \leq n-1$

7 wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer greater
8 than 2, and p_1, p_2, \dots, p_k are distinct random prime numbers, C is a number representative of an

9 encoded form of message word M that is encoded by transforming said message word M to said
10 ciphertext word C whereby,

$$11 \quad C \equiv M^e \pmod{n},$$

12 and wherein e is a number relatively prime to (p_1-1) , (p_2-1) , ..., and (p_k-1) ,

13 said decoding step being performed using a decryption exponent d that is defined by

$$14 \quad d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$$

15 said decoding step including the steps of,

16 (i) defining a plurality of k sub-tasks in accordance with

$$17 \quad M_1 \equiv C_1^{d_1} \pmod{p_1},$$

$$18 \quad M_2 \equiv C_2^{d_2} \pmod{p_2},$$

19 \vdots

$$20 \quad M_k \equiv C_k^{d_k} \pmod{p_k},$$

21
22 where

$$23 \quad C_1 \equiv C \pmod{p_1},$$

$$24 \quad C_2 \equiv C \pmod{p_2},$$

25 \vdots

$$26 \quad C_k \equiv C \pmod{p_k},$$

$$27 \quad d_1 \equiv d \pmod{(p_1 - 1)},$$

$$28 \quad d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

29 \vdots

$$30 \quad d_k \equiv d \pmod{(p_k - 1)},$$

31 (ii) solving said sub-tasks to determine results M_1, M_2, \dots, M_k , and

32 (iii) combining said results of said subtasks in accordance with a fast recursive combining
33 process to produce said message word M in accordance with,

$$34 \quad Y_i \equiv Y_{i-1} + [(M_i - Y_{i-1}) (w_i^{-1} \pmod{p_i}) \pmod{p_i}] \cdot w_i \pmod{n}$$

35 where $2 \leq i \leq k$, and
36

37 $M = Y_k, Y_1 = M_1, \text{ and } w_i = \prod_{j < i} p_j$

38 whereby said step of decoding is accelerated.

1 16. (Three Times Amended) A cryptographic communications system for establishing
2 communications that are backwards compatible with preexisting public key transformation
3 schemes, comprising:

4 a communication medium;

5 encoding means coupled to said communication medium and adapted for transforming a
6 transmit message word M to a ciphertext word C and for transmitting said ciphertext word C on
7 said medium, where M corresponds to a number representative of a message, and

8 $0 \leq M \leq n-1$ where n is a composite number of the form

9 $n = p_1 \cdot p_2 \cdot \dots \cdot p_k,$

10 where k is an integer greater than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers,

11 and where C corresponds to a number representative of an enciphered form of said message, and
12 corresponds to

13 $C \equiv M^e \pmod{n},$

14 where e is a number relatively prime to $(p_1-1), (p_2-1), \dots,$ and (p_k-1) ; and

15 decoding means coupled to said communication medium and adapted for receiving C via
16 said medium and for transforming C to a receive message word M' where M' corresponds to a
17 number representative of a deciphered form of C , said decoding means being operative to
18 perform a decryption process using a decryption exponent d that is defined by

19 $d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$

20 said decryption process including the steps of

21 (i) defining a plurality of k sub-tasks in accordance with,

22 $C_1 \equiv C \pmod{p_1},$

23 $C_2 \equiv C \pmod{p_2},$

24 \vdots

25 $C_k \equiv C \pmod{p_k},$

26 where,

27 $d_1 \equiv d \pmod{(p_1 - 1)},$

28 $d_2 \equiv d \pmod{(p_2 - 1)},$
 29 \vdots
 30 $d_k \equiv d \pmod{(p_k - 1)},$
 31
 32 $M_1' \equiv C_1^{d_1} \pmod{p_1},$
 33 $M_2' \equiv C_2^{d_2} \pmod{p_2}, \text{ and}$
 34 \vdots
 35 $M_k' \equiv C_k^{d_k} \pmod{p_k},$
 36 (ii) solving said sub-tasks to determine results M_1', M_2', \dots, M_k' , and
 37 (iii) combining said results of said subtasks by a fast recursive combining process to
 38 produce said receive message word M' in accordance with
 39 $Y_i \equiv Y_{i-1} + [(M_i' - Y_{i-1}) (w_i^{-1} \pmod{p_i}) \pmod{p_i}] \cdot w_i \pmod{n}$
 40 where $2 \leq i \leq k$ and
 41 $M' = Y_k, Y_1 = M_1,$ and $w_i = \prod_{j < i} p_j,$
 42 wherein $M' = M.$

1 17. (Twice Amended) A method for establishing cryptographic communications that are
 2 backwards compatible with preexisting public key transformation schemes, comprising the steps
 3 of:
 4 encoding a plaintext message word M to a ciphertext word C , wherein M corresponds to
 5 a number representative of a message and wherein
 6 $0 \leq M \leq n-1,$
 7 wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer
 8 greater than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, C is a number
 9 representative of an encoded form of message word M , and wherein said encoding step
 10 comprises transforming said message word M to said ciphertext word C , whereby
 11 $C \equiv M^e \pmod{n},$
 12 and wherein e is a number relatively prime to $(p_1-1), (p_2-1), \dots,$ and (p_k-1) ; and

13 decoding said ciphertext word C to a receive message word M', said decoding step being
14 performed using a decryption exponent d that is defined by

$$15 \quad d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$$

16 said decoding step including the further steps of,

17 defining a plurality of k sub-tasks in accordance with

$$18 \quad M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$19 \quad M_2' \equiv C_2^{d_2} \pmod{p_2},$$

20 \vdots

$$21 \quad M_k' \equiv C_k^{d_k} \pmod{p_k},$$

22 wherein

$$23 \quad C_1 \equiv C \pmod{p_1},$$

$$24 \quad C_2 \equiv C \pmod{p_2},$$

25 \vdots

$$26 \quad C_k \equiv C \pmod{p_k},$$

$$27 \quad d_1 \equiv d \pmod{(p_1 - 1)},$$

$$28 \quad d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

29 \vdots

$$30 \quad d_k \equiv d \pmod{(p_k - 1)},$$

31 solving said sub-tasks to determine results $M_1', M_2', \dots M_k'$, and

32 combining said results of said sub-tasks to produce said receive message word

33 M', wherein $M'=M$.
34

1 22. (Twice Amended) A cryptographic communications system for establishing
2 communications that are backwards compatible with preexisting public key transformation
3 schemes, comprising:
4 a communication medium;

5 encoding means coupled to said communication medium and adapted for transforming a
6 transmit message word M to a ciphertext word C and for transmitting said ciphertext word C on
7 said medium, wherein M corresponds to a number representative of a message, and

8 $0 \leq M \leq n-1$, wherein n is a composite number of the form,

9
$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k$$

10 wherein k is an integer greater than 2 and p_1, p_2, \dots, p_k are distinct random prime
11 numbers, and wherein said ciphertext word C corresponds to a number representative of an
12 enciphered form of said message and corresponds to

13
$$C \equiv M^e \pmod{n},$$

14 wherein e is a number relatively prime to $(p_1-1), (p_2-1), \dots$, and (p_k-1) ; and

15 decoding means communicatively coupled with said communication medium for
16 receiving said ciphertext word C via said medium, said decoding means being operative to
17 perform a decryption process for transforming said ciphertext word C to a receive message word
18 M' , wherein M' corresponds to a number representative of a deciphered form of C , said
19 decryption process using a decryption exponent d that is defined by

20
$$d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$$

21 said decryption process including the steps of

22 defining a plurality of k sub-tasks in accordance with

23
$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

24
$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

25
$$\vdots$$

26
$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

27 wherein

28
$$C_1 \equiv C \pmod{p_1},$$

29
$$C_2 \equiv C \pmod{p_2},$$

30
$$\vdots$$

31
$$C_k \equiv C \pmod{p_k},$$

32
$$d_1 \equiv d \pmod{(p_1 - 1)},$$

33
$$d_2 \equiv d \pmod{(p_2 - 1)},$$

35
 36 $d_k \equiv d \pmod{(p_k - 1)},$
 37 solving said sub-tasks to determine results $M_1', M_2', \dots M_k',$ and
 38 combining said results of said sub-tasks to produce said receive message word M'
 39 whereby $M' = M.$

1 27. (Twice Amended) A method for establishing cryptographic communications that are
 2 backwards compatible with preexisting public key transformation schemes, comprising the step
 3 of:

4 encoding a plaintext message word M to a ciphertext word C , wherein M corresponds to
 5 a number representative of a message, and

6 $0 \leq M \leq n-1,$

7 n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, wherein k is an integer
 8 greater than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, and wherein the ciphertext
 9 word C is a number representative of an encoded form of message word M , wherein said step of
 10 encoding includes the steps of

11 defining a plurality of k sub-tasks in accordance with

12 $C_1 \equiv M^{e_1} \pmod{p_1},$

13 $C_2 \equiv M^{e_2} \pmod{p_2},$

14 \vdots

15 $C_k \equiv M^{e_k} \pmod{p_k},$

16 where

17 $M_1 \equiv M \pmod{p_1},$

18 $M_2 \equiv M \pmod{p_2},$

19 \vdots

20 $M_k \equiv M \pmod{p_k},$

21

22 $e_1 \equiv e \pmod{(p_1 - 1)},$

23 $e_2 \equiv e \pmod{(p_2 - 1)},$ and

24

:

25

$$e_k \equiv e \pmod{(p_k - 1)},$$

26

wherein e is a number relatively prime to $(p_1 - 1)$, $(p_2 - 1)$, ..., and $(p_k - 1)$,

27

solving said sub-tasks to determine results C_1, C_2, \dots, C_k , and

28

combining said results of said sub-tasks to produce said ciphertext word C .

1

32. (Twice Amended) A cryptographic communications system for establishing

2

communications that are backwards compatible with preexisting public key transformation

3

schemes, comprising:

4

a communication medium,

5

encoding means coupled to said communication medium and operative to transform a

6

transmit message word M to a ciphertext word C , and to transmit said ciphertext word C on said

7

medium, wherein M corresponds to a number representative of a message, and

8

$$0 \leq M \leq n-1,$$

9

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$ wherein k is an integer

10

greater than 2 and p_1, p_2, \dots, p_k , are distinct random prime numbers, and wherein the ciphertext

11

word C is a number representative of an encoded form of message word M , said encoding means

12

being operative to transform said transmit message word M to said ciphertext word C by

13

performing an encoding process comprising the steps of

14

defining a plurality of k sub-tasks in accordance with

15

$$C_1 \equiv M_1^{e_1} \pmod{p_1},$$

16

$$C_2 \equiv M_2^{e_2} \pmod{p_2},$$

17

:

18

$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

19

where

20

$$M_1 \equiv M \pmod{p_1},$$

21

$$M_2 \equiv M \pmod{p_2},$$

22

:

23

$$M_k \equiv M \pmod{p_k},$$

24

25

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

26

$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

27

\vdots

28

$$e_k \equiv e \pmod{(p_k - 1)},$$

29

wherein e is a number relatively prime to (p_1-1) , (p_2-1) , ..., and (p_k-1) ,

30

solving said sub-tasks to determine results C_1, C_2, \dots, C_k , and

31

combining said results of said sub-tasks to produce said ciphertext word C .

1 37. (Twice Amended) A method for establishing cryptographic communications that are

2 backwards compatible with preexisting public key transformation schemes, comprising the steps

3 of:

4 decoding a ciphertext word C to a message word M , wherein M corresponds to a number

5 representative of a message and wherein

$$6 \quad 0 \leq M \leq n-1$$

7 wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer greater

8 than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, C is a number representative of an

9 encoded form of message word M that is encoded by transforming said message word M to said

10 ciphertext word C whereby

$$11 \quad C \equiv M^e \pmod{n},$$

12 and wherein e is a number relatively prime to (p_1-1) , (p_2-1) , ..., and (p_k-1) ;

13 said decoding step being performed using a decryption exponent d that is defined by

$$14 \quad d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$$

15 wherein said step of decoding includes the steps of

16 defining a plurality of k sub-tasks in accordance with

$$17 \quad M_1 \equiv C_1^{d_1} \pmod{p_1},$$

$$18 \quad M_2 \equiv C_2^{d_2} \pmod{p_2},$$

19

\vdots

$$20 \quad M_k \equiv C_k^{d_k} \pmod{p_k},$$

21 wherein
 22 $C_1 \equiv C \pmod{p_1},$
 23 $C_2 \equiv C \pmod{p_2},$
 24 \vdots
 25 $C_k \equiv C \pmod{p_k},$
 26
 27 $d_1 \equiv d \pmod{(p_1 - 1)},$
 28 $d_2 \equiv d \pmod{(p_2 - 1)},$ and
 29 \vdots
 30 $d_k \equiv d \pmod{(p_k - 1)},$
 31 solving said sub-tasks to determine results $M_1, M_2, \dots, M_k,$ and
 32 combining said results of said sub-tasks to produce said message word $M.$

1 42. (Twice Amended) A cryptographic communications system for establishing communications
 2 that are backwards compatible with preexisting public key transformation schemes, comprising:
 3 a communication medium;
 4 communicatively coupled with said communication medium for receiving a ciphertext
 5 word C via said medium, and being operative to transform said ciphertext word C to a receive
 6 message word M' , wherein a message M corresponds to a number representative of a message
 7 and wherein,
 8 $0 \leq M \leq n-1$
 9 wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer greater
 10 than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, and wherein said ciphertext word C
 11 is a number representative of an encoded form of said message word M that is encoded by
 12 transforming M to said ciphertext word C whereby,
 13 $C \equiv M^e \pmod{n},$
 14 and wherein e is a number relatively prime to $(p_1-1), (p_2-1), \dots,$ and $(p_k-1);$
 15 said decoding means being operative to perform a decryption process using a decryption
 16 exponent d that is defined by
 17 $d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$

18 said decryption process including the steps of

19 defining a plurality of k sub-tasks in accordance with,

20
$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

21
$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

22
$$\vdots$$

23
$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

24 wherein,

25
$$C_1 \equiv C \pmod{p_1},$$

26
$$C_2 \equiv C \pmod{p_2},$$

27
$$\vdots$$

28
$$C_k \equiv C \pmod{p_k},$$

30
$$d_1 \equiv d \pmod{(p_1 - 1)},$$

31
$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

32
$$\vdots$$

33
$$d_k \equiv d \pmod{(p_k - 1)},$$

34 solving said sub-tasks to determine results M_1', M_2', \dots, M_k' , and

35 combining said results of said sub-tasks to produce said receive message word

36 M' , whereby $M' = M$.

1 47. (Twice Amended) A method for generating a digital signature that is backwards

2 compatible with preexisting public key transformation schemes, comprising the step of:

3 signing a plaintext message word M to create a signed ciphertext word C , wherein M

4 corresponds to a number representative of a message, and

5
$$0 \leq M \leq n-1,$$

6 n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, wherein k is an integer

7 greater than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, and wherein the signed

8 ciphertext word C is a number representative of a signed form of message word M , wherein

9
$$C \equiv M^d \pmod{n}, \text{ and}$$

wherein said step of signing includes the steps of
defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{d_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

wherein d is defined by

$$d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)}, \text{ and}$$

e is a number relatively prime to $(p_1 - 1)$, $(p_2 - 1)$, ..., and $(p_k - 1)$,

solving said sub-tasks to determine results C_1, C_2, \dots, C_k , and

combining said results of said sub-tasks to produce said ciphertext word C .

52. (Twice Amended) A digital signature generation system that is backwards compatible
with preexisting public key transformation schemes, comprising:

a communication medium;

digital signature generating means coupled to said communication medium and operative
to transform a transmit message word M to a signed ciphertext word C , and to transmit said
signed ciphertext word C on said medium, wherein M corresponds to a number representative of
a message, and

$$0 \leq M \leq n-1,$$

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$ wherein k is an integer greater than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, and wherein the signed ciphertext word C is a number representative of a signed form of said message word M, wherein

$$C \equiv M^d \pmod{n},$$

said digital signature generating means being operative to transform said transmit message word M to said signed ciphertext word C by performing a digital signature generating process comprising the steps of,

defining a plurality of k sub-tasks in accordance with,

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{d_k} \pmod{p_k},$$

where,

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

wherein d is defined by,

$$d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)}, \text{ and}$$

e is a number relatively prime to $(p_1 - 1), (p_2 - 1), \dots$, and $(p_k - 1)$,

solving said sub-tasks to determine results C_1, C_2, \dots, C_k , and

combining said results of said sub-tasks to produce said signed ciphertext word C.

1 57. (Twice Amended) A digital signature process that is backwards compatible with
2 preexisting public key transformation schemes, comprising the steps of:

3 signing a plaintext message word M to create a signed ciphertext word C , wherein M
4 corresponds to a number representative of a message and wherein

$$5 \quad 0 \leq M \leq n-1$$

6 wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer
7 greater than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers, C is a number
8 representative of a signed form of message word M , and wherein said encoding step
9 comprises transforming said message word M to said ciphertext word C whereby,

$$10 \quad C \equiv M^d \pmod{n},$$

11 wherein d is defined by

$$12 \quad d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)}, \text{ and}$$

13 e is a number relatively prime to $(p_1 - 1), (p_2 - 1), \dots$, and $(p_k - 1)$; and

14 verifying said ciphertext word C to a receive message word M' by performing the steps

15 of,

16 defining a plurality of k sub-tasks in accordance with

$$17 \quad M_1' \equiv C_1^{e_1} \pmod{p_1},$$

$$18 \quad M_2' \equiv C_2^{e_2} \pmod{p_2},$$

19 \vdots

$$20 \quad M_k' \equiv C_k^{e_k} \pmod{p_k},$$

21 wherein

$$22 \quad C_1 \equiv C \pmod{p_1},$$

$$23 \quad C_2 \equiv C \pmod{p_2},$$

24 \vdots

$$25 \quad C_k \equiv C \pmod{p_k},$$

$$26 \quad e_1 \equiv e \pmod{(p_1 - 1)},$$

$$27 \quad e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

28 \vdots

30

$$e_k \equiv e \pmod{(p_k - 1)},$$

31

solving said sub-tasks to determine results M_1', M_2', \dots, M_k' , and

32

combining said results of said sub-tasks to produce said receive message word

33

M' , whereby $M'=M$.

1 62. (Twice Amended) A digital signature system that is backwards compatible with
2 preexisting public key transformation schemes, comprising:

3 a communication medium;

4 digital signature generating means coupled to said communication medium and adapted

5 for transforming a message word M to a signed ciphertext word C and for transmitting said

6 signed ciphertext word C on said medium, wherein M corresponds to a number representative of

7 a message, and

8 $0 \leq M \leq n-1$, wherein n is a composite number of the form

$$9 \quad n = p_1 \cdot p_2 \cdot \dots \cdot p_k,$$

10 wherein k is an integer greater than 2 and p_1, p_2, \dots, p_k are distinct random prime

11 numbers, and wherein said signed ciphertext word C corresponds to a number representative of a

12 signed form of said message word M and corresponds to

$$13 \quad C \equiv M^d \pmod{n},$$

14 wherein d is defined by

$$15 \quad d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)}, \text{ and}$$

16 e is a number relatively prime to $(p_1-1), (p_2-1), \dots$, and (p_k-1) ; and

17 digital signature verification means communicatively coupled with said communication

18 medium for receiving said signed ciphertext word C via said medium, and being operative to

19 verify said signed ciphertext word C by performing the steps of,

20 defining a plurality of k sub-tasks in accordance with

$$21 \quad M_1' \equiv C_1^{e_1} \pmod{p_1},$$

$$22 \quad M_2' \equiv C_2^{e_2} \pmod{p_2},$$

23 \vdots

$$24 \quad M_k' \equiv C_k^{e_k} \pmod{p_k},$$

25 wherein

26 $C_1 \equiv C \pmod{p_1},$
27 $C_2 \equiv C \pmod{p_2},$
28 \vdots
29 $C_k \equiv C \pmod{p_k},$
30
31 $e_1 \equiv e \pmod{(p_1 - 1)},$
32 $e_2 \equiv e \pmod{(p_2 - 1)},$
33 \vdots
34 $e_k \equiv e \pmod{(p_k - 1)},$
35 solving said sub-tasks to determine results $M_1', M_2', \dots M_k',$ and
36 combining said results of said sub-tasks to produce said receive message word M'
37 wherein $M' = M.$
